REMARKS

Applicants have studied the Office Action dated August 19, 2004. It is submitted that the application, as amended, is in condition for allowance. By virtue of this amendment, claims 1-25 are currently pending in the present application. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks are respectfully requested. In the Office Action, the Examiner:

(6) rejected claims 1-3, 7, 13, 15, 16, 21-23, and 25 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996)," and in further view of Graunke et al (U.S. 5,991,399);

(7) rejected claims 5, 8-12, 14 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996)", in further view of Graunke et al (U.S. 5,991,399) and in further view of Dillon (US 6,351,467);

(8) rejected claims 4 and 6 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996)", and in further view of Graunke et al (U.S. 5,991,399) and in further view of CableVision (Periodical);

(9) rejected claims 17 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996), and further in view of Graunke et al (U.S. 5,991,399) and in further view of Horstmann (U.S. 6,009,401);

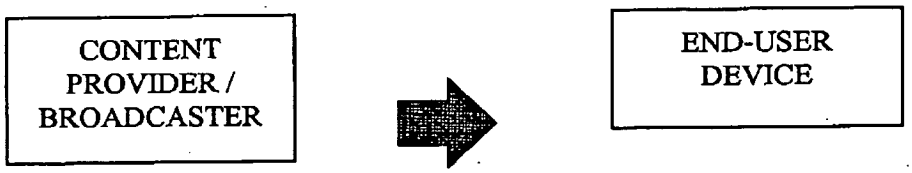
(10) rejected claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Graunke et al (U.S. 5,991,399) and in further view of Horstmann (U.S. 6,009,401); and

(11) rejected claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996), in further view of Graunke et al (U.S. 5,991,399), in further view of Horstmann (U.S. 6,009,401)and in further view of CableVision (periodical).

Overview of the Current Invention

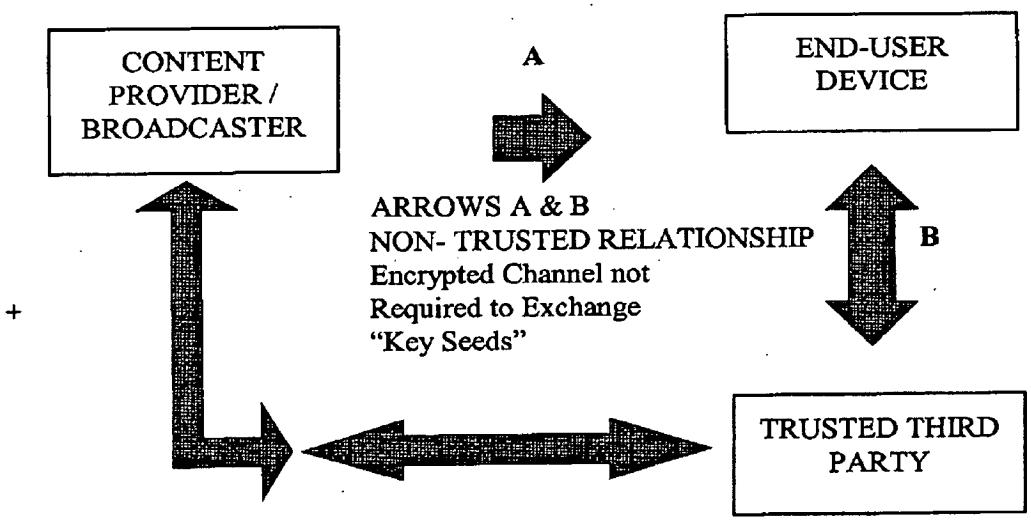
The present invention provides a system, computer readable medium and a method for providing a secure environment for the distribution of digital content. The content rather than the channel

is encrypted for security reasons. This is different than prior art systems that require a trusted relationship between the broadcaster or provider of the content and the user's system through encrypted transport layers.



TRUSTED RELATIONSHIP
In order to Use Key Seeds
Part of Transport Layer is Encrypted To Send Key Seeds

To help illustrate the concept of key management in the present invention the following simplified version of FIG. 6 of the present invention as originally filed is shown.



ONLY ARROW C FROM CONTENT PROVIDER TO TRUSTED THIRD PARTY HAS TO HAVE A PRE-EXISTING TRUST RELATIONSHIP.

The present invention claims a three-way communications between the (i) content provider or broadcaster with (ii) the user's system; and (iii) the trusted third party of the content provider. In order to more particularly point out this feature of "transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key to the trusted third party" then "receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key", the following language has been added to independent claims 1, 7,19, 21, and 25 as follows:

- claims 1, 7, 21, and 25

  transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key to the trusted third party;

  receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

  decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with user's system key;

- claim 19

  a second public key of the user's system;

  a second private key; which corresponds to the second public key;

  re-encryption means for re-encrypting the data decrypting key using the second public key;

  second transferring means for transferring the re-encrypted data decrypting key to the user's system, wherein the user's system possesses the second private key;

  second decrypting means for decrypting the re-encrypted data decrypting key using the second private key; and

  decrypting, on the user's system in a tamper resistant environment, the encrypted data decrypting key with the first private key;

Support for this amendment is found in the present invention as originally filed at least at pages 48-50 as well as FIG. 6. No new matter has been added.

(6) Rejection Under 35 U.S.C. §103(a) applying Dillon '911 in view of Schneier and Graunke

As noted above, the Examiner rejected claims 1-3, 7, 13, 15, 16, 21-23, and 25 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996)" and in further view of Graunke et al (U.S. 5,991,399). Independent claims 1, 7, 21, and 25 have been amended to distinguish over Dillon taken alone and/or in view of Schneier "Applied Cryptography (1996)" and/or in further view of Graunke. As an initial matter, the Dillon '911 reference teaches that the "key seed ID" is sent as opposed to a decrypting key which has been encrypted with a trusted third party. A key seed by its very nature requires a trusted relationship between the sender and recipient, in this case the content provider or broadcaster and the end-user. In the words of Dillon '911 at col. 12, line 9-15 (Emphasis Added):

> *The security of the present invention depends on keeping the "engine private key" private, both within broadcast center 150 and within security engine 130. The engine private key is used to decrypt the account information sent from broadcast center 150 to security engine 130 and should it become known, unauthorized users would gain access to the key seeds needed to decrypt documents.*

This engine private key must be transferred or shared between the broadcast center and the user's system through an encrypted channel. See Dillon '911 at col.6, lines 26-37. Accordingly, a trusted encrypted channel must be established between the broadcaster and user's system to use key seeds. In contrast, the present invention does not require a trusted relationship or encrypted transport layer between the broadcaster and the user's system for exchanging "key seeds." In the words of Dillon at col.8, lines 33-44:

> "In executing function F3, broadcast center 150 periodically, e.g., monthly, sends account status information to each of the plurality of receiving computers, including receiving computer 110. The account information is tailored to the receiving computer and includes a statement of its receiver's status (e.g., satisfactory, overdrawn, limited access, etc.). The account information also includes core information required by security engine 130 to create keys to decrypt electronic documents. Although the account information is broadcast in the clear, the contents

of the account information is encrypted in such a way that only security engine 130 may access and decrypt the account information." (Emphasis Added).

Here Dillon is relying on pre-sending key information to the security engine 130 on a periodic basis so that the security engine 130 is able "to create keys to decrypt electronic documents." The present invention eliminates this step of pre-sending account status information. The present invention does not require a trusted relationship between the user's system and the broadcast center. The present invention operates over unsecure broadcast channels as well as the Internet. Accordingly, independent claims 1, 7, 21, and 25 distinguish over Dillon '911 taken alone and/or in view of Schneier and/or in further view of Graunke for at least this reason.

Continuing further, the present invention achieves it's high level of security between the broadcaster and user's system by transferring the first decrypting key (i.e. the decrypting key for content) which has been encrypted using a trusted third party such as a clearinghouse. Subsequently, the user's system transfers the first decrypting key, which is encrypted by the clearinghouse to the clearinghouse. Next the first decrypting key is re-encrypted with a user's system key. Accordingly, only the user's system receiving the first decrypting key along with the associated encrypted content can access the decrypting key as re-encrypted with the user's system key. This type of use of open broadcast channels for transferring content over unprotected broadcast streams is not taught by Dillon's use of "key seeds." The Examiner goes on to correctly state on page 3 of the Office Action *"Dillon '911 does not specifically disclose a double-encryption technique where a first encrypting key is encrypted using a second encrypted key"* and goes on to combine Dillon '911 with Schneier.[1] The teachings of Schneier taken alone and/or with Dillon's use of key seeds does not solve the underlying technical requirement of a key seed i.e. a secure or encrypted transport layer between the broadcaster and the user's system.

Further, Dillon '911 taken alone and/or in view of Schneier and/or in view of Graunke, are silent on transferring the encrypted first decrypting key, which has been encrypted with the

[1] Applicants make no statement whether such combination is even proper.

second encrypting key to the trusted third party;

receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with the user's system key

Accordingly, independent claims 1, 7, 21, and 25 distinguish over Dillon '911 taken alone and/or in view of Schneier and/or in further view of Graunke for at least this reason as well.

Moreover, the Applicants respectfully submit that the combination of Dillon taken alone and/or in view of Schneier and/or in further view of Graunke *teaches away* from independent claims 1, 7, 21, and 25:

transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key to the trusted third party;

receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with the user's system key;

Schneier at page 176discusses the short comings of "pre-sending" "key-encryption keys" as required in Dillon at col.8, lines 33-44. In the words of Schneier "*key-encrypting keys have to be distributed manually (although they can be secured in a tamperproof device, like a smart card), but only seldomly.*" Again, in the present invention there is no need for this trusted relationship between the content provider or broadcaster and the user's system to "pre-send keys" either manually, through smart cards or otherwise. The present invention works with a public key of the trusted third party, where the trusted third party decrypts the encrypted data encrypting key sent from the user's system and then re-encrypts the data encrypting key with the public key of the user's system. This three way relationship between the (i) content provider or broadcaster with (ii) the user's system; and (iii) the trusted third party of the content provider is no where suggested nor taught by Dillon taken alone and/or in view of Schneier and/or in further view of Graunke. Accordingly, independent claims 1, 7, 21, and 25 distinguish over Dillon '911 taken alone and/or in view of Schneier and/or in further

view of Graunke for at least this reason as well.

Still further, the Examiner goes on to correctly state on page 4 of the Office Action *"Dillon/Schneier does not specifically a tamper resistant environment. Graunke, however, in the abstract and other related test, discloses [...] key management."*.[2] However, Graunke is silent on re-encryption of keys by "transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key to the trusted third party" then "receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key." Accordingly, independent claims 1, 7, 21, and 25 distinguish over Dillon '911 taken alone and/or in view of Schneier and/or in further view of Graunke for at least this reason as well.

For the foregoing reasons, independent claims 1, 7, 19, and 21 have been amended to distinguish over Dillon '911 in view of Schneier and in further view of Graunke. Claims 2-3, 5, 8-16, and 22-24 depend from claims 1, 7, and 21 respectively; since dependent claims contain all the limitations of the independent claims, claims 2-3, 5, 8-16, and 22-24 distinguish over Dillon '911 in view of Schneier and in further view of Graunke as well.

Lastly, with regard to claim 15 as amended recites:

> 15. (Currently Amended) The method as defined in claim 7, wherein the step of receiving the encrypted content data, includes receiving the encrypted content data along with a network address of the trusted third party.

Support for this amendment is found on pages 52-54 of the present invention. No new matter has been added. Dillon '911 taken alone and/or in view of Schneier and/or in view of Graunke are silent on embedding a network address of the trusted third party into the encrypted content data. The present invention allows the content provider or broadcaster to select which trusted third part to use. This way not only one trusted third party provider has to be used for each transaction. Further embedding the network address of the trusted third party in the encrypted content data permits one

[2] Applicants make no statement whether such combination is even proper.

more security check to make sure the source address of the first decrypting key (i.e. the data decrypting key) matches the address of the trusted third party listed in the encrypted content. This level of flexibility and additional security is no where suggested or taught by Dillon '911 in view of Schneier and in further view of Graunke. The Applicants respectfully submit that the Examiner's rejection of claim 15 has been overcome for these reasons as well.

(7) Rejection Under 35 U.S.C. §103(a) applying
Dillon '911 in view of Schneier and Graunke and Dillon ' 467

As noted above, the Examiner rejected claims 5, 8-12, 14 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996)", in further view of Graunke et al (U.S. 5,991,399) and in further view of Dillon (US 6,351,467). Independent claims 1, 7, 21, and 25 have been amended to distinguish over Dillon '911 taken alone and/or in view of Schneier" and/or in view of Graunke and/or in further view of and in further view of Dillon '467.[3]

In regard to claims 5, 12, and 24, DirectPC requires a local security card distributed manually with the user's device as taught by Dillon '911 which is required to correctly handle the "keyseeds". Stated differently every DirectPC system must have an access card i.e. smart card with a security code as the "engine master key" to receive properly decode key seeds. See Dillon '911 and Dillon '697 smart card examples at col. 5, lines 7-21 and Dillon '467 at col. 15, lines 60-62 states only that keys must be provided and is silent on how keys are provided. Further Dillon '467 describes how keys may be provided through a back-end system. Dillon is silent on using a trusted third party to re-encrypt decrypting keys with a user's system key.

Further in regards to claims 8, 9-11, and 14, independent claims 1, 7, and 21 as discussed in the section entitled "(6) Rejection Under 35 U.S.C. §103(a) applying Dillon '911 in view of Schneier

[3] Applicants make no statement whether such combination is even proper.

and Graunke" have been amended to distinguish over all of these combinations including Dillon '467. Schneier at page 176 discusses the short comings of "pre-sending" "key-encryption keys" as required in Dillon at col.8, lines 33-44. In the words of Schneier "*key-encrypting keys have to be distributed manually (although they can be secured in a tamperproof device, like a smart card), but only seldomly.*" Again, in the present invention there is no need for this trusted relationship between the content provider or broadcaster and the user's system to "pre-send keys" either manually, through smart cards or otherwise. The present invention works with a public key of the trusted third party, where the trusted third party decrypts the encrypted data encrypting key sent from the user's system and then re-encrypts the data encrypting key with the public key of the user's system. This three way communications between the (i) content provider or broadcaster with (ii) the user's system; and (iii) the trusted third party of the content provider is no where suggested nor taught by Dillon taken alone and/or in view of Schneier and/or in further view of Graunke. Accordingly, independent claims 1, 7, 21, and 25 distinguish over Dillon '911 taken alone and/or in view of Schneier and/or in view of Graunke and/or in view of Dillon '467 for at least this reason as well.

For the foregoing reasons, independent claims 1, 7, 19, and 21 have been amended to distinguish over Dillon '911 in view of Schneier, in view of Graunke, and further in view of Dillon '497. Claims 5, 8-12, 14 and 24 depend from claims 1, 7, and 21 respectively; since dependent claims contain all the limitations of the independent claims, claims 5, 8-12, 14 and 24 distinguish over Dillon '911 in view of Schneier, in view of Graunke, and in further view of Dillon '497 as well. The Applicants respectfully request that the Examiner's rejection be withdrawn.

(8) Dillon '911 in view of Schneier and Graunke and CableVision

As noted above, the Examiner rejected claims 4 and 6 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996)", and in further view of Graunke et al (U.S. 5,991,399) and in further view of CableVision (Periodical) Independent claim 1 has been amended to distinguish over Dillon '911 taken alone and/or in view of Schneier" and/or in view of Graunke and/or in further view of and in further view of CableVision.

The Examiner goes on to correctly state on page 5 of the Office Action "*Dillon/Schneier/Graunke does not specifically disclose broadcasting promotional data including a schedule of the broadcast time, CableVision teaches that DirectTV and DirectPC...*"[4] However, DirectTV and DirectPC is notoriously well known to require a secure smart card to setup service between the user's system and broadcast system.[5] Schneier at page 176 discusses the short comings of "pre-sending" "key-encryption keys" as required in Dillon at col.8, lines 33-44. In the words of Schneier "*key-encrypting keys have to be distributed manually (although they can be secured in a tamperproof device, like a smart card), but only seldomly.*" Again, in the present invention there is no need for this trusted relationship between the content provider or broadcaster and the user's system to "pre-send keys" either manually, through smart cards or otherwise. The present invention works with a public key of the trusted third party, where the trusted third party decrypts the encrypted data encrypting key sent from the user's system and then re-encrypts the data encrypting key with the public key of the user's system. This three way relationship between the (i) content provider or broadcaster with (ii) the user's system; and (iii) the trusted third party of the content provider is no where suggested nor taught by Dillon taken alone and/or in view of Schneier and/or in further view of Graunke. Accordingly, independent claim 1 distinguish over Dillon '911 taken alone and/or in view of Schneier and/or in view of Graunke and/or in view of Cable Vision for at least this reason as well.

Claims 4 and 6 depend from claim 1; since dependent claims contain all the limitations of the independent claims, claims 4 and 6 distinguish over Dillon '911 in view of Schneier, in view of Graunke, and in further view of CableVision as well. The Applicants respectfully request that the Examiner's rejection be withdrawn.

---

[4] Applicants make no statement whether such combination is even proper.

[5] See for example http://electronickits.com/sat/sat.htm and http://www.dish-network-vs-direct-tv.com/dishnetwork-faq.htm

(9 and 11) Dillon '911 in view of varoius combinations of Schneier, Graunke, Horstmann and CableVision

As noted above, the Examiner rejected claims 17 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996), and further in view of Graunke et al (U.S. 5,991,399) and in further view of Horstmann (U.S. 6,009,401).[6] The Examiner also rejected claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Schneier "Applied Cryptography (1996), in further view of Graunke et al (U.S. 5,991,399), in further view of Horstmann (U.S. 6,009,401)and in further view of CableVision (periodical). The Examiner goes on to correctly state on page 6 of the Office Action *"Dillon/Schneier/Graunke does not specifically disclose a clearing house"* and goes on to combine Dillon/Schneier/Graunke with Horstmann.[7] Horstmann is silent on a clearinghouse used for receiving "the encrypted first decrypting key, which has been encrypted with the second encrypting key to the trusted third party" then transferring "the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key." The CableVision periodical teaches DirectTV which requires an access card as discussed in the section above entitled "(8) Dillon '911 in view of Schneier and Graunke and CableVision". Accordingly, claims 17 and 18 and claim 20 distinguish over Dillon '911 in view of Schneier and Graunke in various combination with Horstmann and CableVision as well.

(10) Dillon '911 in view of Graunke, Dillon '467 and Horstmann

As noted above, the Examiner rejected claims 19 under 35 U.S.C. § 103(a) as being unpatentable over Dillon (U.S. 6,337,911) in view of Graunke et al (U.S. 5,991,399) and in further view of Horstmann (U.S. 6,009,401). Claim 19 has been amended to distinguished over Dillon '911 taken alone and/or in view of Graunke, Dillon '467 and Horstmann. As the Examiner correctly states on *page 3, of the Office Action "Dillon '911 does not disclose double-encryption technique"* and goes

[6]Applicants make no statement whether such combination is even proper.

[7]Applicants make no statement whether such combination is even proper.

on to combine Schneier. The Examiner did not cite Schneier in this rejection. None of the remaining references Graunke, Dillon '467 and Horstmann teach double-encryption techniques. Further, Schneier does not show multiple levels of encryption at a clearing house where the content decrypting key is reencrypted with the key of the user's system. Further, the details of multiple key encryption over broadcast infrastructure using a data decrypting key, a first public key, a first private key, a second public key, a second private key, and re-encrypting the data encrypting key using the second public key at the clearinghouse is simple not shown in the combination proposed by the Examiner. The Applicants respectfully request the Examiner to detail with particularity where each of claimed these elements, as amended, as shown in the each reference cited. This level of detail regarding key structure has not been addressed in any previous claim by the Examiner. [8]

For the foregoing reasons,, claim 19 distinguish over Dillon '911 in view of Graunke, Dillon '467 and Horstmann.

CONCLUSION

The remaining cited references have been reviewed and are not believed to effect the patentability of the claims as amended.

In this Response, Applicants have amended certain claims. In light of the Office Action, Applicants believe these amendments serve a useful clarification purpose, and are desirable for clarification purposes, independent of patentability. Accordingly, Applicants respectfully submit that the claim amendments do not limit the range of any permissible equivalents.

Applicants acknowledge the continuing duty of candor and good faith to disclosure of information

---

[8] If, however, the Examiner's statements are based on facts within the personal knowledge of the Examiner, the Applicant respectfully requests that the Examiner support these references by filing an affidavit as is allowed under MPEP §707 citing 37 CFR 1.104(d)(2) to place this prosecution record in a better condition for appeal on at least this point alone.

known to be material to the examination of this application. In accordance with 37 CFR § 1.56, all such information is dutifully made of record. The foreseeable equivalents of any territory surrendered by amendment is limited to the territory taught by the information of record. No other territory afforded by the doctrine of equivalents is knowingly surrendered and everything else is unforeseeable at the time of this amendment by the Applicants and their attorneys.

Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's Office Action have been overcome, and that all claims in the application are allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if this would expedite the prosecution of this application.

Respectfully submitted.

November 19, 2004 By:_____

Jon A. Gibbons (Reg. No. 37,333)
Attorney for Applicants
Fleit, Kain, Gibbons, Gutman,
Bongini & Bianco P.L.
One Boca Commerce Center, Suite 111
551 Northwest 77th Street
Boca Raton, FL 33487
Telephone: (561) 989-9811
Facsimile: (561) 989-9812

Please direct all correspondence to Customer Number 23334

150-a99-164amd#3.wpd